

Overview of Cybersecurity in India

Vinayak Godse

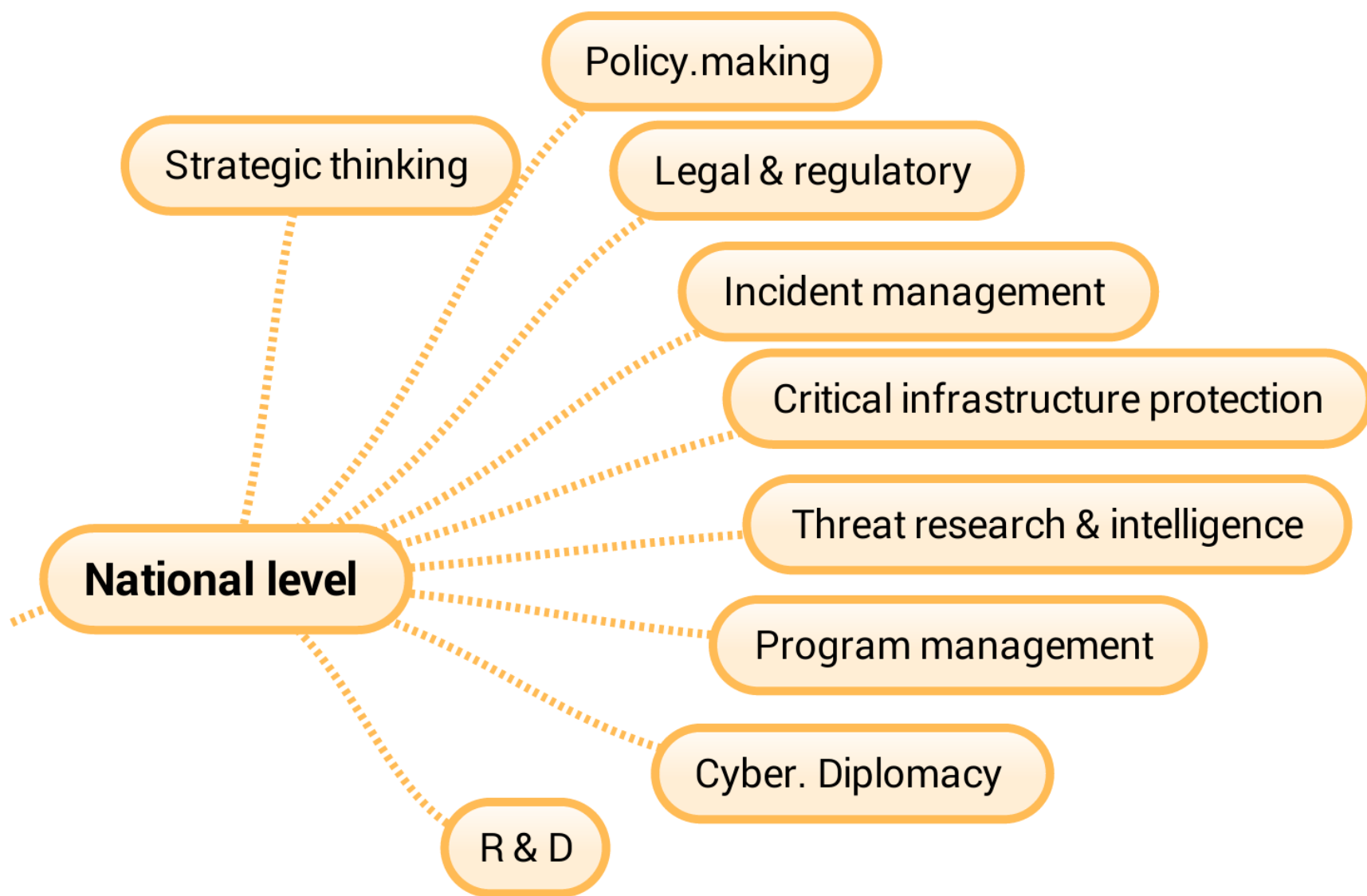
Director, Data Protection

Data Security Council of India

September 15, 2014

1:30 pm to 3:00 pm

Cyber Security: National Efforts



National Cyber Security Policy [NCSP]

Creating a Secure Cyber Ecosystem

Human Resource Development

Creating an Assurance Framework

Information Sharing and
Cooperation

Strengthening Regulatory Framework

Developing Effective Public
Private Partnerships

Protection & Resilience of Critical
Information Infrastructure (CII)

Reducing Supply Chain Risks

Creating Mechanisms for Security
Threat Early Warning, Vulnerability
Mgt & Response

Creating Cyber Security Awareness

Encouraging Open Standards

Securing e-Governance Services

Prioritized Approach for
Implementation

Promotion of R&D in Cyber Security



NCSP: 14 objectives, 14 Strategic areas and 50+ activities

Legal Framework for Cyber Security

Cyber crime | Illegal activities | Legal rights

Definition of entities, corresponding regulatory measures

Intermediaries | Corporate | Citizens

Cyber contraventions & Cyber crime

*Definitions | Civil proceedings | Criminal code
Penalties | Punishments*

Admissibility of electronic evidence

Legal recognition of electronic records

Regulatory infrastructure, facilitator and their empowerment

Incident response | Investigation | Judicial

Responsibility & Accountability of Corporate

Expectations | Diligence | Penalties

Critical Infrastructure protections & legal provisions

Notification | Authority | Penalties | Terrorism

Access to information, investigation support

Authority | Process | Obligations

Retention & preservation of information

Data type | Retention period | Obligations

Content regulations, Blocking public access

Content Standards | Authority | Obligations

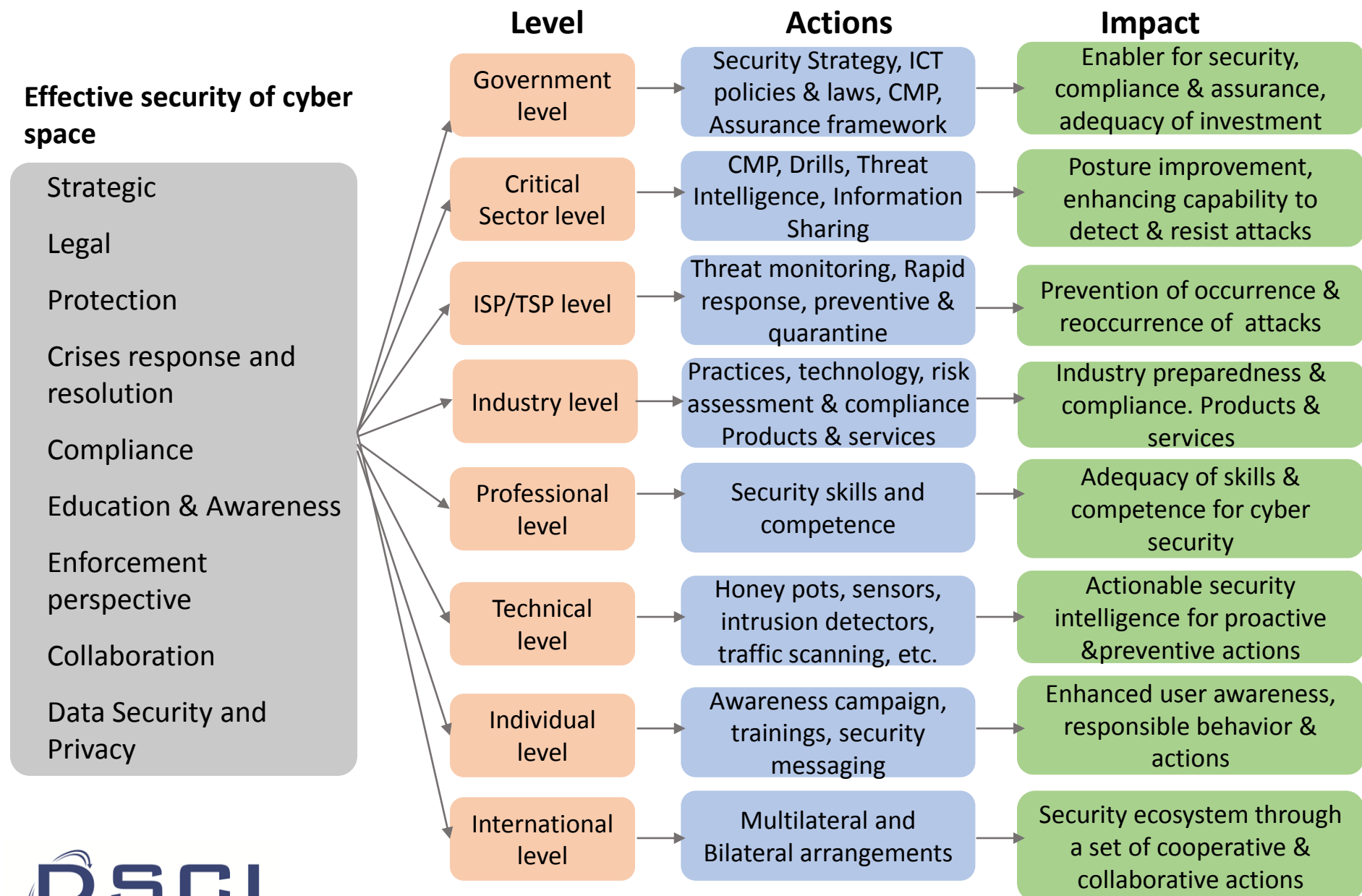
Lawful Interceptions & monitoring

Agencies | Empowerment | Due processes

Abetment of offense, attempt to commit offense

Civil proceedings | Criminal code

Actions for Cyber Security



Key Initiatives

Setting up 'Joint Working Group' for public private partnership in cyber security

Led by National Security Council Secretariat (NSCS), which works under guidance of National Security Advisor

Proposed setting up 'National Cyber Coordination Centre (NCCC)'

To be led by Ministry of Communication and IT

Setting up 'National Critical Information Infrastructure Protection Centre (NCIIPC)'

*A special agency for protection of Critical Information Infrastructure Protection
.. Published a guidelines for critical sector organization*

Recognition as an authorizing nation under Common Criteria Recognition Arrangement (CCRA)

India recently acquired a state of authorizing nation

Information Security Education and Awareness Program (ISEA)

Graduate, post-graduate and PhD programs as well as awareness initiatives

Opportunities

“Availability of skilled resources and expertise” for the global cyber security requirements

India IT industry offers “security consulting & services” to the global clients

Prolonged “experience of delivering critical services” to the desired quality and scale

India is emerging as a “hub for research and development” of cyber security products

“Security product ecosystem” in the country is emerging very fast

Thank You